	Application No.	Applicant(s)
Notice of Allowability	09/740,411	CHEN ET AL.
	Examiner	Art Unit	
	Aravind K Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *14 March 2005*.

2. ☒ The allowed claim(s) is/are *1-10*.

3. ☒ The drawings filed on *28 June 2001* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some*   c) ☐ None of the:

        1. ☐ Certified copies of the priority documents have been received.

        2. ☐ Certified copies of the priority documents have been received in Application No. _____ .

        3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

    * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

    (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

        1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____ .

    (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of

    Paper No./Mail Date _____ .

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)

2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)

3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____

4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material

5. ☐ Notice of Informal Patent Application (PTO-152)

6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .

7. ☐ Examiner's Amendment/Comment

8. ☒ Examiner's Statement of Reasons for Allowance

9. ☐ Other _____ .

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

DETAILED ACTION

1. This is in response to the amendment filed on 14 March 2005.

2. Claims 1-10 are pending in the application.

3. Claims 1-10 have been allowed.

Response to Arguments

4. Applicant's arguments, see pages 7-16, filed 14 March 2005, with respect to claims 1-10 have been fully considered and are persuasive. The rejection of the claims has been withdrawn.

Allowable Subject Matter

5. Claims 1-10 are allowed.

The following is an examiner's statement of reasons for allowance.

As to independent claims 1, 3 and 5, prior art does not disclose, teach or fairly suggest the step of providing a signal representing the constant, C, which is equal to 2^{+2mk} mod N. Prior art does not disclose, teach or fairly suggest the step of multiplying the value A by the constant C using a circuit which accepts two input operands and which produces an output result value Zo given by $A\ C\ 2^{-mk}$ modulo N. Prior art does not disclose, teach or fairly suggest the step of storing the value Zo in a first register and in a second register. Prior art does not disclose, teach or fairly suggest the step for sequential values of an index i running from 1 to t, repeatedly using the value in the second register as both of the operands for the circuit, with the output of the circuit being stored back into the second register and, when e_{t-i}, is 1, using again the contents of the second register as one input operand to the circuit with the other input operand being the Zo value in the first register with the output of the circuit being stored in the first register. Prior art does not disclose, teach or fairly suggest the step of upon completion of the repetition, operating

the circuit with the contents of the second register as one input operand with the constant 1 as the

other input operand. Prior art does not disclose, teach or fairly suggest the step of storing the

output of the circuit in at least one of the registers, whereby the at least one register contains the

binary representation of A^E modulo N. Prior art does not disclose, teach or fairly suggest the

step of providing a binary signal representing the constant, C, which is equal to 2^{+2mk} mod N.

Prior art does not disclose, teach or fairly suggest the step of multiplying the value A by the

constant C using a circuit which accepts two input operands and which produces an output result

value Zo given by A C 2^{-mk} modulo N. Prior art does not disclose, teach or fairly suggest the

step of storing the value Zo in a first register. Prior art does not disclose, teach or fairly suggest

the step that if eo = 1, storing the value 1 in a second register, otherwise storing the contents of

the first register in the second register. Prior art does not disclose, teach or fairly suggest the step

for sequential values of an index i running from 1 to t, repeatedly using the value in the second

register as both of the operands for the circuit, with the output of the circuit being stored back

into the second register and, when e_{t-i}, is 1, using again the contents of the second register as one

input operand to the circuit with the other input operand being the Zo value in the first register

with the output of the circuit being stored in the first register. Prior art does not disclose, teach

or fairly suggest the step of upon completion of the repetition, operating the circuit with the

contents of the second register as one input operand with the constant 1 as the other input

operand. Prior art does not disclose, teach or fairly suggest the step of storing the output of the

circuit in at least one of the registers, whereby the at least one register contains the binary

representation of AE modulo N. Prior art does not disclose, teach or fairly suggest the step of

repeatedly operating, for at most t cycles, a circuit which computes F G 2^{-mk} modulo N for binary

input operands F and G to the circuit, with the circuit inputs being controllably selected, during

each repetition, from the constant 1, the constant 2^{+2mk} modulo N and the previous output from

the circuit so as to produce an output of $A^{E} 2^{+2mk}$ modulo N. Prior art does not disclose, teach or

fairly suggest the step of operating the circuit with one input being the output from the repeated

step and the other input being the constant 1, whereby the output of the circuit, after at most t

cycles, is A^{E} modulo N.

The closest prior art to the current application was Monier U.S. Patent No. 5,764,554.

The current application differs from Monier U.S. Patent No. 5,764,554 in all the six recited claim

steps. In the applicants' first claim step, there is provided a signal representing a constant which

is equal to a particular power of 2 modulo N which is typically a large prime number employed

in modular arithmetic operations. In contrast, the portion of the Monier patent teaches the

production of a parameter that has a different exponent for the base 2. Furthermore, the modular

parameter is N' in Monier where $N = N' * 2^{a}$ (see Monier column 6, lines 4-9). Additionally, the

presence of a subscript 1 in the expression H_l suggests that H is a parameter that varies with an

index. In contrast, it is seen that: applicants' recited constant C is indeed a constant that does not

depend upon any index value that indicates a particular iteration point. Most relevantly, however,

the constant that applicants provide has a different exponent for the base 2. Moreover, it is to be

particularly noted that in applicants' claim the value mk is not equal to n, but is greater than or

equal to n+2. In applicants' step 2, there is a multiplication step in which the value A is

multiplied by the constant provided in step 1. The value of A referred to in applicants' claim 1 is

the base value, which is going to be raised to the exponent E. The output of applicants' step 2 is a

value Zo given by $A C 2^{-mk}$ modulo N. In stark contrast, the referenced citation to column 1, line

50 of the patent to Monier is not even a multiplication step but is instead merely the computation

of a parameter. In particular, it is seen that the parameter H is not the same as the parameter C as

employed by the present applicants (see the discussion above with respect to applicants' claim

step 1). Furthermore, the multiplication operation referred to in column 7, line 30 is a

multiplication not by the total number of bits in the variable C but is rather a multiplication using

only a portion of this variable. In this regard, it is noted that C in the patent to Monier refers to

one of his input variables. In particular, it is the variable for which he seeks modulo N reduction.

In contrast, in applicants' claim 1, the symbol C is used to refer to a constant parameter that is

equal to 2^{+2mk} mod M. Accordingly, it is seen that, even though there is an allusion to a

multiplying operation in the cited portion of the Monier patent, the things that are multiplied are

significantly different. In applicants' claim step 3, there is a recitation to storing the value Zo in

a first register and also in a second register. In stark contrast, it is seen that Monier refers to the

loading of only a single register. Furthermore, applicants' claim step 3 refers to a step in which

the value Zo is stored. In stark and utter contrast, Monier refers instead to storing only a portion

of the variable C. Accordingly, it is seen that not only are the same variable quantities not being

stored but also Monier incorporates only a storage into a single register. Clearly, the operations

recited are not only different but are significantly different. In applicants' claimed step 4 in claim

1, there is a recitation of an iterative process. This iterative process refers to certain bits, e, where

the values of the variable a represent bits in the exponent F. In stark contrast, the only similarity

between applicants' claim step 4 and Monier is that there is an iterative process described.

However, nowhere in the cited portions of the patent to Monier is there any indication that the

cited process or steps include anything whatsoever that could even remotely be construed as an

exponent E. Furthermore, it is indicated that applicants' claim step 4 refers to a circuit. In

particular this circuit is a multiplying circuit. However, in there is not one reference whatsoever

to a multiplying operation. There is a reference to a possible division operation wherein the

divisor is an exponent of the base 2. However, as is well known, such operations are typically

carried out as right shift operations. Thus, Monier refers to a division operation, not to a

multiplication operation. Applicants' fifth claim step refers to an operation that occurs upon

completion of the iteration step of claim 4. In applicants' recited step, it refers to the operation of

the multiplying circuit. This circuit is employed with specific inputs. In short, applicants' claim

step 5 is, in effect, a multiplication operation. However in contrast, when one views the patent to

Monier upon which the Examiner relies, one is faced not with a multiplication operation but one

in which the least significant word of a particular value is ignored with the remaining portion

being loaded into a particular register. This is not in any sense the operation of a multiplying

circuit modulo N. Applicants' claim step 6 refers to the operation of storing the output of the

multiplying circuit in one of the registers. Furthermore, applicants' "whereby clause" asserts that

the value that is stored in this register is a binary representation of A^E modulo N. In short, the

output that is stored in one of the registers represents an exponentiation modulo N. Again in

stark contrast, the patent is not directed to modular exponentiation at all but rather to modular

reduction. This is the final step in his process. In this regard, it is noted that Monier himself

describes Figure 3 as a flow chart of "the modular reduction method in one embodiment of the

present invention". Modular reduction is not the same as modular exponentiation. They are

significantly different operations. Additionally, while applicants' sixth claimed step refers simply

to a storing operation, the cited portion of the patent to Monier refers to an addition operation for the values of C. Again, storage is not the same as addition.

As to independent claims 6 and 7, prior art does not disclose, teach or fairly suggest a circuit having two input operands for signals representing binary numbers F and G and which produces as a result the binary representation $F \, G \, 2^{-mk}$ modulo N. Prior art does not disclose, teach or fairly suggest a first register for providing constants 2^{+2mk} modulo N and 1 as the input operands to the circuit. Prior art does not disclose, teach or fairly suggest a second register means for storing output from the circuit. Prior art does not disclose, teach or fairly suggest means for controlling input operand selection to the circuit so that after at most t iterations, the output result of the circuit is A^E modulo N (figure 1, elements 23 and 24). Prior art does not disclose, teach or fairly suggest a modular multiplication circuit having two inputs operands for signals representing binary numbers F and G and which produces as a result the binary representation $F \, G \, 2^{-mk}$ modulo N. Prior art does not disclose, teach or fairly suggest a first multiplexor for selecting input signals for a first one of the input operands to the modular multiplication circuit. Prior art does not disclose, teach or fairly suggest a second multiplexor for selecting input signals for second one of the input operands to the modular multiplication circuit. Prior art does not disclose, teach or fairly suggest a first output register. Prior art does not disclose, teach or fairly suggest a second output register. Prior art does not disclose, teach or fairly suggest a selector circuit for supplying output from the modular multiplication circuit to either one or both of the firs and second registers. Prior art does not disclose, teach or fairly suggest means for controlling the first and second multiplexors and the selector circuit over repeated cycles to produce the A^E modulo N value in at least one of the output registers.

The closest prior art to the current application was Monier U.S. Patent No. 5,764,554. The current application differs from Monier U.S. Patent No. 5,764,554 in that Monier does not produce modulo exponentiation results. Monier is solely directed to modulo reduction operations not exponentiation. This patent characterizes Figure 1 as "a schematic view of a circuit enabling the performance of a modular operation according to the Montgomery Method." However, the patent to Monier characterizes the circuits shown in Figure 1 in a more specific manner beginning in column 1, lines 48-49, wherein it states that the "modular reduction method implemented by the circuit in Figure 1 includes the following stages . . ..". Clearly, in the mind of Monier, the circuit shown in Figure 1 is a method for modular reduction. As pointed out above, modular reduction is not the same as modular exponentiation. The only place whatsoever where exponentiation is mentioned in the patent to Monier is in regard to its use in the RSA algorithm. Nowhere is there anything whatsoever talk about a specific method for carrying out modular exponentiation. Nowhere in Monier's Figure 1 is there any teaching, disclosure or suggestion that a particular signal path, register, multiplexor, multiplier, delay or storage circuit accepts, employs, uses, produces or otherwise manipulates a variable that could be described as an exponent such as E in applicants' Figure 20 and as recited in applicants' claim 6. Furthermore, to the extent that Monier describes any kind of a finite state machine, it is clearly and unequivocally not a finite state machine that accepts as an input the value E as shown in applicants' Figure 2 and as recited in applicants' claims. Applicants' claims are directed to an apparatus for performing modular exponentiation. Monier only alludes to modular exponentiation but does not describe a process for it. The patent to Monier is specifically limited to a process for modular reduction. This is not the same process as modular exponentiation.

The dependant claims, being further limiting to the independent claims, definite and enabled by the specification are also allowed.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

6.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
March 30, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100